BY ORDER OF THE COMMANDER
341ST SPACE WING

AIR FORCE INSTRUCTION 31-401

341ST SPACE WING
Supplement 1

1 OCTOBER 2000

Security

MANAGING THE INFORMATION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the Malmstrom Electronic Publication Distribution Library (MEPDL) WWW site at: http://www.malmstrom.af.mil/pdo/pubs.html. If you lack access, contact your Base Publications Manager.

OPR: 341 SFS/SFAI (SSgt Ingles) Certified by: 341 SFS/CC (Lt Col Anderson)
Supersedes AFI 31-401/MAFB Sup 1, 28 May 1996. Pages: 7
Distribution: F

The OPR for this supplement is 341 SFS/SFAI. This supplement implements and extends the guidance of Air Force Instruction (AFI) 31-401, ***Information Security,*** and applies to all personnel assigned to the 341ST Space Wing and subordinate units, and personnel assigned or attached to, or supported by, Malmstrom AFB.

SUMMARY OF REVISIONS

This supplement updates AFI 31-401/MAFB Sup 1, 28 May 1996 in its entirety. A bar (|) indicates a revision from previous editions.

1.3.5.1. Unit commanders or staff agency chiefs will notify the 341 SFS/SFAI, by letter, upon appointment of a new security manager. The primary or alternate security manager will have at least 1 year retainability on station from the time of appointment. The 341 SFS/SFAI will provide training to all security managers. Within 10 duty days after appointment, security managers must contact 341 SFS/SFAI to set up an appointment for training.

1.4.2. The Installation Security Program Manager (ISPM), through their representatives, conduct annual Information Security Program Reviews (ISPR) with each agency assigned to Malmstrom AFB. As a minimum, reviews consist of Top Secret Control Account (TSCA) procedures, unit's DoD Unclassified Controlled Nuclear Information program, sampling of classified for which the ISPM representatives have the appropriate security clearances, training programs, all security related paperwork and forms, Personnel Security requirements, reproduction and destruction procedures, and Classification Management procedures.

1.4.2.1. These reviews may cover other areas at the discretion of the ISPM representatives.

1.4.3. Unit commanders or staff agency chiefs must review and coordinate on all ISPR reports. These reports will then be maintained in the Security Manager's Handbook.

1.4.3.1. Security managers may not perform self-inspections on their own programs. Self-inspection reports must be coordinated by the unit commander or staff agency chief and posted in the Security Manager's Handbook.

1.4.4. The Base Entry/Exit Inspection Program. Will be conducted by the 341 SFS/SFO and will include a check for unauthorized entry or removal of classified information.

2.1.3. The 341 SW/CC is the only Original Classification Authority (OCA) approved for Malmstrom.

2.1.3.1. 341 SFS/SFAI personnel will brief OCA into the program. Refresher training will be conducted annually.

2.3.1. Coordinate all challenges to classification with the OCA and 341 SFS/SFAI.

2.3.4. If the challenge involves reasonable doubt about level of classification, safeguard the information at the higher level of classification pending a determination by OCA.

3.3.1. Coordinate requests for mandatory declassification review of information classified by OCA with 341 SFS/SFAI.

5.4. Strict compliance with Top Secret control procedures always takes precedence over administrative convenience.

5.6.1.2. 341 SFS/SFAI must be made aware of any release of classified information to retired general officers at least 3 duty days prior to the release. This notification will include the level of classified to be released and the names, social security numbers, and department or agency of prior employment of the retired general officers to whom the material will be released.

5.10.1. A TSCA is established when an activity routinely originates, stores, receives, or transmits Top Secret information. Top Secret material may not be permanently received by an activity unless a TSCA has been formally established and a Top Secret Control Officer (TSCO) has been appointed. The unit commander or staff agency chief formally establishes the TSCA by letter. Maintain this letter with the account, and provide a copy to 341 SFS/SFAI.

5.10.1.1. Unit commanders provide 341 SFS/SFAI with a copy of the TSCO appointment letter. 341 SFS/SFAI will provide training for all TSCOs NLT 60 days after appointment.

5.10.1.1.1. Unit commanders may designate persons other than TSCOs to pick up Top Secret message traffic from telecommunications facilities. These persons must have a Top Secret clearance. Also, they must be briefed by the TSCO or alternate on proper storage and transportation requirements.

5.10.1.2.1. Keep the Air Force Form 144, **Top Secret Access Record and Cover Sheet**, with the material at all times and remove it when the material is destroyed, downgraded, or declassified. Do not remove it when the material is transferred to another TSCA.

5.10.1.3.1. Inventory officials need not physically sight each Top Secret document stored at a Missile Alert Facility (MAF). The inventory official must contact each appropriate MAF to ensure the material is on-hand and properly accounted for via an Air Force Form 614, **Charge Out Record**, in lieu of traveling to each MAF.

5.14.1. In the event an aircraft carrying classified lands unplanned at Malmstrom AFB or Great Falls International Airport, 341 SFS/SFAI will be contacted for storage guidance. If the aircraft is transporting Special Compartmented Information (SCI) or material that cannot be removed from the aircraft, the

Chief, Security Forces will provide the level of security requested by the aircraft commander or senior Defense Courier Service representative.

5.17.1. Security managers are responsible for approval, control, and development of copying procedures for each copier in their unit that reproduces classified material. All copiers will be posted with the applicable visual aid, warning whether or not classified reproduction is authorized. All reproduction of classified must be kept to a minimum and is only authorized to meet mission requirements. All personnel must be aware that sending classified material over a secure fax constitutes reproduction.

5.19. Requests to use a non-General Services Administration (GSA) approved container, for classified storage, must be approved by 341 CES locksmith and 341 SFS/SFAI. A local civilian locksmith may not approve the use of non-GSA approved containers for classified storage. Security Managers will maintain a list of all containers used for classified storage assigned to their unit. Include in the list the assigned container number or symbol, location of the container (i.e. room and building number), level of material stored within the container, and primary container custodian and phone number.

5.20.4. The 341 CS/SCBA will provide temporary storage for classified material up to and including Secret for transient personnel. The 341 CS will not provide temporary storage for Top Secret materials at anytime. During normal duty hours, Secret material will be taken to the Base Information Transfer Center vault, located in Building 300. During nonduty hours, weekends, or holidays, classified material up to and including Secret will be taken by transient personnel to the Malmstrom Command Post (MCP), Building 500, for temporary storage. Top Secret material requiring temporary storage, at anytime, to include duty hours, nonduty hours, weekends, or holidays will be taken by transient personnel to the MCP, Building 500. If personnel are TDY to Malmstrom AFB on an official visit, they may use either of the procedures above or they may store their classified with the agency they are visiting, provided the agency is capable of storing classified material to the appropriate level. In the event an individual arrives with SCI, contact 341 SFS/SFAI personnel immediately. At no time will SCI material be stored in a non-SCI approved facility.

5.20.5. Personnel assigned to base operations, base entry points, and billeting offices must be knowledgeable of the repository locations and how to contact designated repository custodians during duty or nonduty hours.

5.22.3. The following procedures apply to all facilities used for unattended or open storage of classified:

5.22.3.1. The owner or user agency security manager must:

5.22.3.1.1. Use the design criteria outlined in Military Handbook (MILHDBK) 1013/1A and related provisions within this supplement to construct or modify facilities.

5.23.3.1.2. (Added) Review and coordinate all requests for unattended or open storage facilities prior to submission to 341 SFS/SFAI. As a minimum, requests must include classification and type of material requiring storage to include special access requirements, complete description of the area (including floor plan, present type of alarm system, if any, and location), complete justification for the request, (i.e., size and amount of classified, and reasons storage containers cannot be used).

5.23.3.1.3. (Added) Maintain a copy of all related correspondence, including letters of request, survey reports, work order requests, approvals, etc.

5.23.3.1.4. (Added) Coordinate all modifications through 341 SFS/SFAI. Keep 341 SFS/SFAI apprised of proposed modifications and invite them to all preconstruction planning.

5.23.3.2. (Added) A representative of 341 SFS/SFAI will:

5.23.3.2.1. (Added) Schedule and conduct an initial survey along with the appropriate civil engineer representative to evaluate the design criteria and administrative procedures for existing or future facilities using the criteria outlined in MILHDBK 1013/1A. Modifications to existing facilities or occupation by a different activity require a new survey to ensure security integrity has not been downgraded.

5.23.3.2.3. (Added) Coordinate all related documentation with 341 CES/CEOE.

5.23.3.2.4. (Added) Process all related documentation through the installation commander.

5.23.3.2.5. (Added) Maintain a copy of all related correspondence, including letters of request, survey reports, work order requests, approvals and disapprovals, etc.

5.23.3.2.6. (Added) Annually reinspect all facilities where waivers were granted.

5.23.3.3. (Added) A representative of 341 CES/CEOE will accompany the 341 SFS/SFAI to:

5.23.3.3.1. (Added) Provide technical assistance during completion of all surveys to determine if facilities meet or exceed the design criteria as outlined in MILHDBK 1013/1A.

5.23.3.3.2. (Added) Endorse all survey reports using one of the following guidelines:

5.23.3.3.2.1. (Added) Provide certification the facility meets design criteria of MILHDBK 1013/1A.

5.23.3.3.2.2. (Added) Provide certification that although the facility design standards are not in compliance with MILHDBK 1013/1A, the physical security provided by the existing design and construction provides protection equal to or greater than MILHDBK 1013/1A standards.

5.23.3.3.2.3. (Added) Agree with any recommendations of 341 SFS/SFAI or provide additional recommendations.

5.23.4.4. (Added) When classified Automated Data Processing (ADP) is requested within the area, a computer security representative accompanies 341 SFS/SFAI and 341 CES/CEOE representatives to provide technical assistance and recommendations for ADP security requirements.

5.23.5. (Added) The approval and waiver authority for Malmstrom AFB is the installation commander. They will:

5.23.5.1. (Added) Direct upgrade actions as necessary if they are not satisfied with the recommendations of 341 SFS/SFAI and 341 CES/CEOE.

5.23.5.2. (Added) Authorize waivers of design criteria and approve facilities based on recommendations provided by 341 SFS/SFAI and 341 CES/CEOE.

5.23.6. (Added) Any modifications to approved facilities must be coordinated with 341 SFS/SFAI and revalidated by 341 SW/CC, as determined by 341 SFS/SFAI.

5.23.7.2. (Added) All facilities used for unattended or open storage of classified material not meeting the design criteria of MILHDBK 1013/1A must be approved in writing by 341 SW/CC. Design criteria are verified through completion of the survey required below. Send requests for unattended or open storage areas to 341 SFS/SFAI.

5.23.8. (Added) Classified Discussion Areas. Send requests for recurring classified discussion areas to the 341 SFS/SFAI. This supplement will be used as guidance for all classified discussion areas used for classified discussions, meetings, training sessions, seminars, etc., conducted on a recurring basis. All

facilities designated as a classified discussion area will be approved and administratively processed (i.e., requests, surveys, waivers, approvals, etc.) using the same procedures for establishing an unattended or open storage area as outlined above. The decision to establish a classified discussion area is made by unit commanders or staff agency chiefs with the concurrence of the ISPM based on the frequency of classified discussion. (Examples: Areas or rooms used for mass briefings, training sessions, conferences, or work areas where routine classified discussion is essential to mission accomplishment such as command posts, SIOP-ESI training areas, and missile trainer facilities.)

5.23.8.2. (Added) Consideration must be given to protecting the area between any false and true ceilings. The installation commander, after consultation with the ISPM, and civil engineer representative, determines if alarm coverage in this area is necessary. This decision is based on several factors including, but not limited to nature and level of classified discussion to occur within the facility, hostile intelligence threat to the installation, location of the facility within the installation, construction of the facility, location of the discussion area within the facility, and present security operations, visitor control, etc.

5.23.8.3. (Added) Consideration must be given to removal of all telephones and intercom type systems within classified discussion areas. Where determined necessary by 341 SFS/SFAI, these systems must be equipped with "push-to-talk" handsets or similar devices designed to preclude inadvertent access to surrounding discussions.

5.23.8.4. (Added) The ISPM will determine if an inquiry is warranted when the facility is found insecure, established key control procedures fail, or evidence of surreptitious entry exists.

5.23.8.5. (Added) The owner or user agency is responsible for initiating requests under the Technical Surveillance Countermeasures Program, based on a recommendation from 341 SFS/SFAI.

5.24.1. Although 341 CES locksmith may have a security clearance, they will not be allowed access to classified while performing repair or maintenance on security containers. Whenever a locksmith is performing any type of repair or maintenance on a security container used to store classified, the locksmith must be under constant surveillance of the container custodian or other authorized representative. Whenever possible, remove all classified from the security container before a locksmith performs repair or maintenance. At no time will a local civilian locksmith be allowed access to classified information.

5.29.1. All shredders and destruction equipment will be posted with the applicable Air Force Visual Aid. Always use a “secure volume” when shredding classified. This is done by shredding unclassified material having the same characteristics as the classified (i.e., color, texture, etc.) along with classified.

5.29.2.6.1. Agencies that store classified materials in or for other agencies must enter into a formal written agreement. Each commander or staff agency chief must sign this agreement and both units will maintain a copy.

6.7.1.1. As a minimum, each Air Force member or employee must have verbal authorization from his or her supervisor to escort or hand-carry classified material outside his or her normal work center. Written authorization is not required for individuals traveling in government owned vehicles to or from missile sites.

6.7.2. Individuals required to pass through an entry or exit inspection point other than base gates will be provided written authorization. This authorization is normally in the form of a DD Form 2501, **Courier Authorization Card.**

6.9.1. Approval for Transporting Classified aboard Commercial Aircraft. The local ISPM must approve and provide guidance for all authorizations to transport classified information aboard commercial aircraft. This approval may be verbal.

7.1. ISPM, in coordination with each Special Access Program Manager, will determine the need for their representatives access to any Special Access Program information. This includes, but is not limited to, Critical Nuclear Weapon Design Information (CNWDI), Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI), and North Atlantic Treaty Organization (NATO) information.

8.9. Unit commanders or staff agency chiefs must have active indoctrination and recurring training programs that outline responsibilities for supervisors and security managers. This is normally accomplished through use of formal Operating Instructions (OI) but may also be in the form of checklists. This plan is designed to discourage use of the "read and initial" method as the only way to conduct security education and training. It is also designed to meet security education requirements that equal the needs of the personnel and the unit or staff agency. Consider Communication Security, Physical Security, Personnel Security, Computer Security, Operations Security, Classification Management, Information Security, and so forth. Additionally, training will be outline by calendar quarter on what training is planned for the unit and how it will be accomplished.

8.8.3. Security managers are responsible for providing assigned personnel with foreign travel briefings.

9.2.1. Report all actual or possible security violations to the 341 SFS/SFAI.

9.3.2.3. All inquiry officials will contact 341 SFS/SFAI to set up a briefing within 24 hours after appointment.

9.4.1.4. Once an inquiry is completed, the inquiry official will provide the 341 SFS/SFAI a complete original copy of the inquiry report. 341 SFS/SFAI will review the report for completeness, attach a technical review, and forward the report to the appointing authority for concurrence. All security violation reports will be sent to the installation commander for information.

9.4.2. Notify 341 SFS/SFAI when a breach in security occurs during transmission, regardless of who the sender is.

9.5.1. Responsible unit commanders, with coordination with 341 SFS/SFAI, conduct inquiries as appropriate.

9.5.1.1. 341 SW/CC, in coordination with the ISPM and AFOSI, will conduct a damage assessment when the compromise of information originally classified by them is reasonably expected to cause damage to national security. This damage assessment will be in writing and include identification of the source, date, and circumstances of the compromise, classification of the specific information lost or compromised, an analysis and statement of the known or probable damage to national security, an assessment of the possible advantages to foreign powers, an assessment of the appropriate administrative, disciplinary, or legal actions associated with the compromise.

9.5.1.2. Any notification to an agency outside the control of the 341 SW regarding Security Violations, including Damage Assessments, will be coordinated with 341 SFS/SFAI. In the event an individual who has had access to classified material is on unauthorized absence, an inquiry as appropriate under the circumstances, to include consideration of the length of the absence and the degree of sensitivity of the classified material involved, shall be conducted to detect if any indications of activities, behavior, or associations exist that may be harmful to the interest of national security.

9.5.1.3. 341 SW/CC notifies all known holders of changes resulting from the assessments described above.

9.6.2. Generally, inquiry officials will have 10 duty days to complete the inquiry and report. The appointing official and 341 SFS/SFAI will approve extensions. This approval may be verbal; however, a request letter must follow within 2 duty days. All originals and duplicates of inquiry or formal investigation reports will be maintained by 341 SFS/SFAI.

THOMAS F. DEPPE, Colonel, USAF
Commander